Training Course on iOS Device Forensics, Deep Dumps and Artifacts

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This advanced training course provides an in-depth exploration of iOS device forensics, equipping participants with cutting-edge methodologies for data acquisition, deep dump analysis, and comprehensive artifact recovery from Apple's highly secure ecosystem. Participants will gain critical expertise in navigating the complexities of iOS operating systems, including bypassing advanced security features and performing forensically sound extractions from locked, encrypted, and physically damaged iPhones and iPads. Through extensive hands-on labs and real-world case scenarios, this program empowers digital forensic specialists to uncover hidden evidence, analyze intricate user activities, and present court-admissible findings from iOS devices.

Training Course on iOS Device Forensics, Deep Dumps and Artifacts focuses on unearthing elusive data from full file system dumps, deciphering encrypted backups and keychains, and interpreting the vast array of iOS application artifacts. With the continuous evolution of Apple's security protocols and the increasing prevalence of mobile cybercrime, this course delivers the essential knowledge and practical skills to stay ahead in the dynamic field of digital investigations. Graduates will be proficient in leveraging both commercial and open-source forensic tools, understanding APFS file system intricacies, and developing custom approaches for challenging iOS forensic cases, ensuring they can tackle even the most sophisticated mobile forensic challenges.

Programme Curriculum

Training Course on iOS Device Forensics, Deep Dumps and Artifacts

Introduction

This advanced training course provides an in-depth exploration of iOS device forensics, equipping participants with cutting-edge methodologies for data acquisition, deep dump analysis, and comprehensive artifact recovery from Apple's highly secure ecosystem. Participants will gain critical expertise in navigating the complexities of iOS operating systems, including bypassing advanced security features and performing forensically sound extractions from locked, encrypted, and physically damaged iPhones and iPads. Through extensive hands-on labs and real-world case scenarios, this program empowers digital forensic specialists to uncover hidden evidence, analyze intricate user activities, and present court-admissible findings from iOS devices.

Training Course on iOS Device Forensics, Deep Dumps and Artifacts focuses on unearthing elusive data from full file system dumps, deciphering encrypted backups and keychains, and interpreting the vast array of iOS application artifacts. With the continuous evolution of Apple's security protocols and the increasing prevalence of mobile cybercrime, this course delivers the essential knowledge and practical skills to stay ahead in the dynamic field of digital investigations. Graduates will be proficient in leveraging both commercial and open-source forensic tools, understanding APFS file system intricacies, and developing custom approaches for challenging iOS forensic cases, ensuring they can tackle even the most sophisticated mobile forensic challenges.

Course Duration

10 Days

Course Objectives

1. Execute advanced iOS data acquisition techniques, including full file system extractions and deep dumps from various device states.
2. Perform APFS file system analysis, identifying critical forensic artifacts and understanding its copy-on-write mechanisms.
3. Utilize specialized tools and techniques to effectively bypass iOS security features and access protected data.
4. Conduct in-depth iOS keychain decryption and analysis to recover stored credentials and sensitive information.
5. Analyze and interpret a wide range of iOS application artifacts, including deleted data and hidden communications.
6. Investigate iCloud backups and synced data, understanding their forensic value and acquisition challenges.
7. Perform manual artifact carving and reconstruction from raw iOS deep dumps to recover unparsed data.

8. Understand and apply techniques for iOS malware detection and basic analysis of malicious applications.
9. Reconstruct user timelines and activities using location data, Siri artifacts, and system logs from iOS devices.
10. Develop Python scripts for automated parsing and analysis of complex iOS forensic artifacts.
11. Generate forensically sound reports and provide expert testimony based on robust iOS digital evidence.
12. Adapt forensic strategies to continually evolving iOS versions and emerging security updates.
13. Apply chain of custody principles and best practices for the integrity and admissibility of iOS digital evidence.

Organizational Benefits

1. Superior Investigative Capabilities: Empower teams to conduct thorough and successful investigations involving iOS devices, regardless of complexity.
2. Enhanced Data Recovery Success Rates: Maximize the ability to extract crucial evidence from highly secure and encrypted Apple devices.
3. Reduced Reliance on External Services: Develop in-house expertise, saving costs and time associated with third-party forensic specialists.
4. Proactive Cyber Threat Identification: Gain insights into iOS vulnerabilities and attack vectors to strengthen organizational cybersecurity posture.
5. Improved Compliance & Legal Preparedness: Ensure adherence to legal and regulatory requirements for digital evidence handling and reporting.
6. Accelerated Incident Response: Shorten the time to investigate and contain incidents stemming from iOS devices.
7. Protection of Sensitive Information: Recover and analyze data related to intellectual property theft or data exfiltration via iOS devices.
8. Strategic Advantage: Stay ahead of adversaries by understanding the latest iOS security advancements and forensic countermeasures.
9. Professional Growth & Retention: Invest in highly specialized training for employees, boosting morale and retaining top talent.
10. Evidence Admissibility: Increase the likelihood of digital evidence from iOS devices being accepted in legal proceedings.

Target Participants

- Digital Forensic Examiners
- Law Enforcement Investigators
- Cybersecurity Incident Responders
- E-Discovery Professionals
- IT Security Auditors
- Military and Intelligence Analysts

- Corporate Fraud Investigators
- Digital Forensics Lab Technicians
- Legal Professionals (handling digital evidence)
- Reverse Engineers and Malware Analysts

Course Outline

Module 1: iOS Architecture & Security Fundamentals (iOS Forensics Basics)

- Overview of iOS Operating System Architecture
- Understanding Apple's Security Model (Secure Enclave, Data Protection)
- Device States: Locked, Unlocked, Disabled, and Their Forensic Impact
- Legal & Ethical Considerations in iOS Device Seizure and Examination
- **Case Study**: Initial assessment of a locked iPhone for potential data access.

Module 2: Advanced iOS Data Acquisition Methods (iOS Data Extraction Techniques)

- Logical vs. File System vs. Physical Extractions: In-depth Comparison
- Utilizing Advanced Forensic Tools for Full File System Dumps (Checkm8-based tools, commercial solutions)
- Understanding and Leveraging iTunes/Finder Backups and Sync Data
- Dealing with Pairing Records and Trust Certificates for Acquisition
- **Case Study**: Performing a full file system extraction from a passcode-locked iOS device.

Module 3: APFS File System Analysis (APFS Forensics)

- Deep Dive into Apple File System (APFS) Structures
- Understanding Snapshots, Clones, and Space Management in APFS
- Recovering Deleted Data and Unallocated Space on APFS Volumes
- Interpreting APFS Metadata and Journaling for Timelines
- **Case Study**: Recovering deleted documents from an APFS-formatted iPad.

Module 4: iOS Backup & Cloud Data Forensics (iCloud Forensics & Backups)

- Analyzing Encrypted and Unencrypted iTunes/Finder Backups
- Decrypting iOS Backups and Keychain Data from Backups
- Understanding iCloud Sync Data and its Forensic Implications
- Acquisition Challenges and Strategies for iCloud Data
- **Case Study**: Extracting and decrypting WhatsApp data from an iCloud backup.

Module 5: iOS Keychain & Encryption Decryption (iOS Keychain Analysis)

- The iOS Keychain: Structure, Purpose, and Forensic Value
- Techniques for Extracting and Decrypting Keychain Items
- Recovering Passwords, Wi-Fi Credentials, and Application Tokens
- Understanding Hardware Encryption and Data Protection Classes (DPC)
- **Case Study**: Recovering stored passwords for web services from an extracted keychain.

Module 6: iOS Application Artifact Analysis (iOS App Forensics)

- In-depth Examination of iOS Application Sandboxing
- Identifying and Parsing Application-Specific Databases (SQLite)
- Analyzing Plist Files, Caches, and Other App Data Structures

- Extracting Data from Deleted and Third-Party Applications
- **Case Study**: Reconstructing messages and attachments from a deleted messaging app.

Module 7: Deep Dump & Manual Artifact Carving (iOS Deep Dump Analysis)

- Understanding Raw NAND Dumps and Their Significance
- Techniques for Manual Data Carving from Unparsed Sectors
- Identifying File Headers and Footers for Custom Carving
- Reconstructing Fragmented Files and Deleted Database Entries
- **Case Study**: Carving a partially overwritten photo from a raw iOS dump.

Module 8: Location, Time, and Geolocation Forensics (iOS Geolocation Forensics)

- Analyzing GPS Data, Cell Tower Locations, and Wi-Fi Access Points
- Extracting and Interpreting Core Location Database Artifacts
- Understanding Significant Locations and Frequent Locations Data
- Reconstructing User Movement and Timelines with Geolocation Evidence
- **Case Study**: Mapping a suspect's movements based on location artifacts.

Module 9: Communication & Web Artifacts (iOS Communication Forensics)

- Forensic Analysis of SMS, iMessage, and Call History
- Extracting Data from Popular Messaging Applications (WhatsApp, Signal, Telegram)
- Analyzing Safari Browser History, Downloads, and Search Queries
- Recovering Deleted Communications and Web-Related Data
- **Case Study**: Uncovering deleted conversations from an iMessage thread.

Module 10: iOS System Logs & Device Events (iOS System Forensics)

- Analyzing System Logs, Crash Logs, and Diagnostic Data
- Interpreting Device Connections, Pairing Events, and Power Cycles
- Identifying User Activity via System Usage Data (KnowledgeC Database)
- Forensic Value of Notifications, Siri Usage, and Spotlight Searches
- **Case Study**: Reconstructing a timeline of device usage and specific events.

Module 11: iOS Malware Analysis & Threat Detection (iOS Malware Forensics)

- Identifying Signs of Compromise and Malicious Activity on iOS
- Basic Techniques for iOS Malware Static and Dynamic Analysis
- Understanding Side-Loading, Jailbreaking Threats, and MDM Bypasses
- Detecting Spyware and Monitoring Software on iOS Devices
- **Case Study**: Identifying indicators of compromise from a suspected iOS malware infection.

Module 12: Advanced Anti-Forensics & Countermeasures (iOS Anti-Forensics)

- Recognizing Data Wiping, Encryption, and Anti-Forensic Tools on iOS
- Detecting Jailbreak Attempts and Other Device Tampering
- Bypassing "Stolen Device Protection" and Other New Security Features
- Strategies for Dealing with Damaged or Partially Functioning Devices
- **Case Study**: Analyzing a device where anti-forensic measures were attempted.

Module 13: Scripting for iOS Forensics (Python for iOS Forensics)

- Introduction to Python for Automating Forensic Tasks
- Parsing Custom iOS Artifacts with Python Libraries

- Developing Scripts for Data Extraction and Visualization
- Leveraging Open-Source Tools and APIs for iOS Analysis
- **Case Study**: Building a Python script to parse a unique iOS application's database.

Module 14: Forensic Reporting & Expert Testimony (iOS Forensic Reporting)

- Best Practices for Documenting iOS Forensic Examinations
- Crafting Clear, Concise, and Defensible Forensic Reports
- Understanding Legal Requirements for Digital Evidence Admissibility
- Preparing for and Delivering Effective Expert Witness Testimony
- **Case Study**: Creating a mock forensic report for a simulated iOS investigation.

Module 15: Capstone Project: Comprehensive iOS Investigation (iOS Forensics Capstone)

- End-to-End Simulated iOS Device Investigation Scenario
- Applying all Acquired Skills from Acquisition to Reporting
- Troubleshooting Complex Forensic Challenges
- Presentation of Findings and Expert Recommendations
- **Case Study**: A full-scale investigation of a challenging iOS device, incorporating all learned modules.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com